AMENDMENTS TO THE CLAIMS

Please AMEND claims 1, 2, 5, 10, 12, 18, 22, 23, 25 and 26 in accordance with the following:

1. (Currently Amended) An apparatus for encrypting/decrypting a real-time input stream, comprising:

a control unit ~~receiving~~ configured to receive a data stream of bytes wherein the data stream is an MPEG data stream or a Digital Satellite Service (DSS) data stream, ~~converting~~ convert the data stream into data blocks, ~~providing~~ provide the data blocks for encryption or decryption, ~~receiving~~ receive encrypted or decrypted data blocks, ~~converting~~ convert the received encrypted or decrypted data blocks into bytes, and ~~outputting~~ output the bytes, wherein the control unit generates a start key signal when a new round key is needed;

a key schedule unit ~~providing~~ configured to provide a round key for every round in accordance with the start key signal and an input key having a variable size to provide the round key for the encryption or decryption for each round, wherein the input key size is one of 128, 192, and 256 bits; and

a block round unit ~~receiving~~ configured to receive converted data blocks from the control unit, ~~receiving~~ receive the round key from the key schedule unit, ~~encrypting~~ encrypt or ~~decrypting~~ decrypt the received data blocks, and ~~providing~~ provide the encrypted or decrypted data blocks to the control unit,

wherein the key schedule unit selects a 128 bit round key to the block round unit for the each round using a key register having a capacity of {(size of an inputted block)*(size of one

round)}.

2. (Currently Amended) The apparatus of claim 1, wherein the control unit ~~comprising~~comprises:

an input buffer ~~storing~~ configured to store the data stream of bytes and ~~converting~~ convert the received data stream into the data blocks having a predetermined size so as to output the converted data blocks to the block round unit; and

an output buffer ~~receiving~~ configured to receive the data blocks encrypted or decrypted in the block round unit and ~~converting~~ convert the received data blocks into bytes ~~the byte units~~ so as to output a converted data.

3. (Previously Presented) The apparatus of claim 2, wherein the block round unit completes all round calculation of data having been currently encrypted or decrypted before a next data block is inputted from the control unit and then stores the corresponding result in the output buffer of the control unit.

4. (Cancelled)

5. (Currently Amended) The apparatus of claim 1, wherein the key schedule unit ~~comprising~~comprises:

a key expansion unit ~~expanding~~ configured to expand the inputted key value into a size amounting to {block size*(count of rounds +1)}; and

a key selection unit ~~selecting~~ configured to expand the 128 bit key required for each round from the expanded key value so as to provide the selected key to the block round unit.

6-8. (Cancelled)

9. (Previously Presented) The apparatus of claim 1, wherein the control unit generates a control signal to produce the selected 128 bit round key every round and then outputs the control signal to the key schedule unit.

10. (Currently Amended) An apparatus for encrypting/decrypting a real-time input data stream wherein the data stream is an MPEG data stream or a Digital Satellite Service (DSS) data stream, comprising:

a control unit ~~receiving~~ configured to receive a data stream in first data format, ~~converting~~ convert the data stream and outputting data in a second data format for encryption or decryption, wherein the control unit generates a start key signal when a new round key is needed;

a key schedule unit in communication with the control unit and ~~providing~~ configured to provide a round key for every round in response to the start key signal and an input key having a variable size for the encryption or decryption for each ~~round~~ round, wherein the input key size is one of 128, 192, and 256 bits; and

a block round unit in communication with the control unit and the key schedule unit and ~~receiving~~ configured to receive converted data in second data format from the control unit, ~~receiving~~ receive the round key value from the key schedule unit for encryption or decryption of

each round, and ~~providing~~ provide the encrypted or decrypted result to the control unit,

wherein the key schedule unit expands the input key into a size of {second data format size * (count of rounds +1)}, selects an N bit key required for each round from the expanded key value, and provides the selected N bit key to the block round unit for each round, and

~~wherein~~ the key schedule unit ~~comprises~~ selects a 128 bit round key to the block round unit for the each round using a key register having a capacity of {(size of an inputted block)*(size of one round)}.

11. (Previously Presented) The apparatus of claim 10, wherein the first data format is in bytes, and the second data format is a data block.

12. (Currently Amended) The apparatus of claim 10, wherein the control unit ~~comprising~~comprises:

an input buffer ~~storing~~ configured to store the data stream of the first data format and ~~converting~~ convert the received data stream into the data of the second data format having a predetermined size; and

an output buffer ~~receiving~~ configured to receive data in the second data format and ~~converting~~ convert the data into the first data format.

13. (Original) The apparatus of claim 12, wherein the block round unit substantially completes all data encryption or decryption processing before a next set of data is inputted from the control unit and stores the corresponding result in the output buffer of the

control unit.

14-17. (Cancelled)

18. (Currently Amended) The apparatus of claim 10, wherein the N bit key is equal to ~~a~~ the 128 bit round key.

19-20. (Cancelled)

21. (Previously Presented) The apparatus of claim 10, wherein the control unit generates a control signal to produce the round key in every round.

22. (Currently Amended) A real-time encryption/decryption apparatus, comprising:

a control unit ~~receiving~~ configured to receive a data stream in first data format wherein the data stream is an MPEG data stream or a Digital Satellite Service (DSS) data stream, ~~converting~~ convert the data stream and ~~outputting~~ output data in a second data format for encryption or decryption, wherein the control unit generates a start key signal when a new round key is needed;

a key schedule unit in communication with the control unit and ~~providing~~ configured to provide a round key in a predetermined period in response to the start key signal and an input key having a variable size, wherein the input key size is one of 128, 192, and 256 bits, and ~~wherein~~ the key schedule unit has a key register capable of processing the input key required for

the predetermined period; and

a block round unit in communication with the control unit and the key schedule unit and ~~receiving~~ configured to receive converted data in second data format from the control unit, and ~~receiving~~ receive the round key from the key schedule unit for encryption or decryption of each round,

wherein a size of the key register is no less than {(second data format size)*(size of one period)}.

23. (Currently Amended) The apparatus of claim 22, wherein the first data format is in bytes, and the second data format is ~~in~~ a data block.

24. (Cancelled)

25. (Currently Amended) A method of controlling a data protection key, the method being processed in an encryption apparatus, comprising:

generating a start key signal when a generation of a new data key is needed in the encryption apparatus;

generating a new data key according to [[a]] the start key signal, the new data key generated according to at least one of a predetermined period and a scheduled period in the encryption apparatus, wherein the scheduled period depends on a change of size of the new data key ~~size~~;

~~checking validity of the data key;~~ and

encrypting data corresponding to the period with the new data key in the encryption apparatus[[,]].

~~wherein the start key signal is transmitted for generating the data key.~~

26. (Currently Amended) The method of claim 25, further comprising a data key valid signal provided with the new data key for encryption [[and]] or decryption.

27. (Previously Presented) The method of claim 25, wherein the data are encrypted according to the start key signal in real time.